様式Ｃ－１９

科学研究費助成事業（科学研究費補助金）研究成果報告書

平成 25 年 6 月 3 日現在

機関番号：１２６１２
研究種目：若手研究（B）
研究期間：2010～2012
課題番号： 22760270
研究課題名（和文） 高速通信ネットワークの実現に向けたマルチユーザ通信路符号化の基礎理論の構築
研究課題名（英文） Development of Fundamental Theory on Multi-User Channel Coding for High Speed Network
研究代表者
八木　秀樹（YAGI HIDEKI）
電気通信大学・大学院情報理工学研究科・准教授
研究者番号：60409737

研究成果の概要（和文）：
マルチユーザ通信システムにおいて，最適符号が達成できる符号化レートの解析と，符号化レートの理論限界に迫る符号化法の開発を目的とする．特に，理論上重要な多重アクセス通信路に対し，以下の３つの利点を有する符号の具体的構成法を与えた：(1) 符号長 N の多項式の計算量で実行可能，(2) 漸近的に符号化レートの限界値を達成可能，(3) 復号誤り率が N の指数関数的に減少する．また，有限な符号長の最適符号の符号化レートを解析し，従来より厳密な上界式及び下界式を導出した．

研究成果の概要（英文）：
This study aims to analyze coding rates of optimal codes and to develop methods for constructing codes that can approach the theoretical limit over multi-user communication systems. The main result is to develop an explicit construction method of codes having the following three properties over a (compound) multiple access channel: (1) they can be implemented with the complexity polynomial in the code length N, (2) they can approach the optimal coding rates asymptotically, and (3) their decoding error probability can converge to zero exponentially in N. Another important result is to give bounds on coding rates of optimal codes with a fixed code length N, which are tighter than known bounds.

交付決定額

（金額単位：円）

	直接経費	間接経費	合　計
2010 年度	300,000 円	90,000 円	390,000 円
2011 年度	400,000 円	120,000 円	520,000 円
2012 年度	600,000 円	180,000 円	780,000 円
総　計	1,300,000 円	390,000 円	1,690,000 円

研究分野：工学
科研費の分科・細目：通信・ネットワーク工学
キーワード：マルチユーザ情報理論，通信路符号化，多重アクセス通信路，情報セキュリティ

１．研究開始当初の背景

近年の通信システムの大規模化・高速化に伴い，通信路を複数のユーザで共有し情報を伝送するマルチユーザ通信システムの重要性が増している．例えば，通信衛星から多数の基地局に対して放送を行う場合(**ブロードキャスト通信路**)や，逆に各基地局から通信衛星に向かって同時にデータを伝送する場合(**多重アクセス通信路**)などが，主な具体例として挙げられる．L 対 M マルチユーザ通信路は，L 個の送信機（符号器）と M 個の受信機(復号器)からなる通信路である(図 1)．

各符号器においてメッセージが送信系列に**符号化**され，符号化された系列が一斉に通信路に入力される．通信路では物理的な影響により，送信系列が確率的なひずみを受ける．L 個の復号器はそれぞれの受信系列から送信メッセージを推定する．この操作を**復号**と呼ぶ．

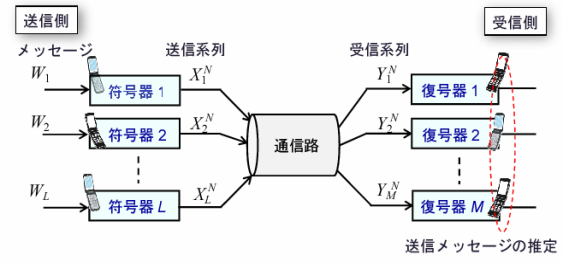

図１．　L 対 M マルチユーザ通信システム

情報通信の信頼性は送信メッセージの**復号誤り率**によって評価される．また，情報通信の効率性は**符号化レート**と呼ばれる送信シンボル当たりで表現されるメッセージのビット長により測られる．『各復号器の復号誤り率を任意に小さくできる符号化・復号法が存在する符号化レートの領域』は**通信路容量域**と呼ばれる．マルチユーザ通信路符号化では，様々なマルチユーザ通信路に関する以下の 2 点が主要な研究課題となる：

(1) 通信の信頼性を確保したまま効率性をどこまで上げられるか（通信路容量）を明らかにすること

(2) 通信路容量（もしくは既知の理論限界）を達成する実用可能な符号化手法を開発すること

マルチユーザ通信では，（1 対 2 や 2 対 2 の通信路など）シンプルな通信路においても通信路容量域が容易に求まらない場合が多い．また，すでに通信路容量域が求められている通信路において，通信路容量を達成し，かつ実用的な計算時間（符号長 N の多項式オーダの計算量）で実現できる符号化方式に関する研究は多くない．既に様々な特性の通信路において理論限界が示され，実用的な計算時間で実現可能な符号が多数開発されてきた単一ユーザ通信路に比べ，マルチユーザ符号化システムの理論的基盤の構築が望まれている．本研究では，基本的なマルチユーザ通信路における符号化問題に焦点を合わせ，上記の課題を解決することを試みた．

２．研究の目的

始めに，基本的な通信路モデルとして，2 対 1 多重アクセス通信路と 2 対 2 マルチユーザ通信路に注目する．2 対 2 マルチユーザ通信路は，各復号器が両符号器からのメッセージを復号する場合，**複合多重アクセス通信路**と呼ばれ，各復号器が 1 つの符号器からのメッセージのみを復号する場合，**干渉通信路**と呼ばれる．干渉通信路は，無線 LAN 環境などの無線ネットワークをモデル化したマルチユーザ通信路と見なせ，理論的な性能の保証は工学的に重要である．

単一ユーザ通信では，通信路容量以下の任意の符号化レートに対し，復号誤り率を任意に小さくできる**構成的な符号構成法**が知られている．復号誤り率 Pe は符号長 N とある正数 $E>0$ を用いて $Pe \le \exp\{-NE\}$ のように上界できることが示されている．これは誤り率 Pe が符号長 N の増大に従って指数的に小さくなることを意味する．一方，マルチユーザ通信では，もっとも基本的な（複合）多重アクセス通信路においてもこのような結果は導かれていない．（複合）多重アクセス通信路の通信路容量域の解析では，ランダムに構成された符号(ランダム符号) の集合を考え，その集合の中に任意に復号誤り率を小さくできる符号が存在することが示された．一方，このような符号の具体的な構成法はほとんど示唆されない．このような背景から，本研究の具体的な目標を以下のように挙げる．

【研究の目的】

（複合）多重アクセス通信路・干渉通信路等の主要なマルチユーザ通信路において，

(1) 通信路容量に迫る構成的な符号化の開発．

(2) 符号長 N の多項式オーダーの計算量で済む，実用的な復号アルゴリズムの開発．

３．研究の方法

(1) 2 対 1 多重アクセス通信路における多項式時間で復号可能な符号化法の開発

2 対 1 多重アクセス通信路において，符号長 N の多項式オーダの計算時間で符号化・復号化が実現可能な符号を検討した．研究代表者が先に開発した符号構成法により，符号化過程の計算量とメモリ量は符号長の多項式オーダの計算量に抑えられることが分かった．しかし，通信路容量の可到達性の証明では系列単位の復号誤り率 Pe を最小にする**最尤復号**を利用したが，最尤復号は符号長 N の指数オーダの計算量を必要とし，このことが実用化の際の大きな問題となる．

単一ユーザ通信路では，この点を解決する**連接符号化**の手法が知られており，実際の通信・記録システムでも利用されている．連接符号化とは，メッセージをまず**外部符号**と呼ばれる代数的アルゴリズムで復号可能な符

号（例えば，Reed-Solomon 符号）により符号化し，外部符号の符号語シンボルを**内部符号**と呼ばれる低計算量で最尤復号が実行できるくらい短い符号長の符号で符号化する，組合せ的符号化法である．本ステップでは，単一ユーザ通信路における連接符号化をマルチユーザ通信路へ拡張し，符号長 N の多項式オーダの計算量で復号が実行できる符号化を検討した．また，構成した符号化方法の誤り率と計算量の評価を行った．マルチユーザ通信路における連接符号化では外部符号と内部符号の組合せ方に任意性がある．そこで，性能が向上する有効な組み合わせ法を検討した．

(2) マルチユーザ通信路における多項式時間で復号可能な符号化法の拡張

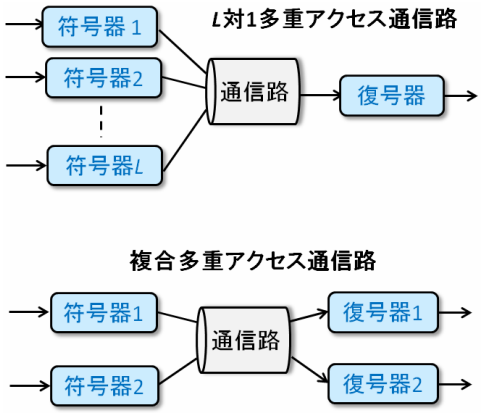

図 2.　拡張した多重アクセス通信路

ステップ(1)の結果を元に，符号器数を増やした L 対 1 多重アクセス通信路や 2 対 2 複合多重アクセス通信路において，符号長 N の多項式オーダ時間で符号化・復号化が実現可能な符号を検討する（図 2）．ステップ(1)で開発する 2 対 1 多重アクセス通信路における符号構成法により，復号化計算量とメモリ量は符号長の多項式オーダの計算量に抑えられることが期待される．一方，符号器数を増やした場合，または復号器が複数存在する場合において，復号の多段性による性能劣化をできる限り抑えられる復号アルゴリズムを検討した．さらに，近年の符号理論における結果を導入し，復号アルゴリズムの計算量のさらなる低減を図る．具体的には，符号長 N の線形（1 次多項式）オーダで全体の復号が実行できるよう検討する．

(3) 多重アクセス通信路における有限ブロック長の最適符号の性能評価

近年，単一ユーザ通信路において**有限長**の符号化を仮定した元で達成可能な符号化レートと復号誤り率のトレードオフ関係を明らかにする研究が注目されている．従来の情報理論では，符号長 N が任意に大きくできる（**無限長**の）状況下で，平均復号誤り率 Pe が目標値 $\varepsilon>0$ 以下になる符号の最大符号化レートを解析した．この最適値は**ε −通信路容量**と呼ばれている．一方，ε −符号化問題の有限長解析では，ブロック長 N を固定した元で，このような符号の最大符号化レートを解析する．

本研究では，マルチユーザ通信において，ε −符号化問題の有限長解析を試みる．初期ステップとして多重アクセス通信路を仮定し，従来知られている最適符号のレートの上界式及び下界式の改善を検討した．これにより，符号長が有限の状況下で達成できる符号化レートがどのように変わるかを調べることができる．

4．研究成果

(1) 2 対 1 多重アクセス通信路における多項式時間で復号可能な符号化法の開発

2 つの符号器と 1 つの復号器から構成される多重アクセス通信路に対して，連接符号化に基づき，符号長 N の多項式オーダの符号化・復号化計算量で通信路容量域の任意のレートを達成できる符号化方法を開発した．この符号化では，まず内部符号は従来型のランダムに構成する符号アンサンブルから適当なものを選ぶことを仮定した[雑誌論文 5]．また，構成した符号の復号誤り率 Pe の上界式を導き，通信路容量域内の符号化レートであれば誤り率が符号長に対して指数関数的に 0 へ収束することを示した．また，このときの指数的速度（**誤り指数**）の具体的な関数形も与えている．提案した符号構成法により，符号化レートの理論限界値を達成し，かつ低計算量で実用できる符号を準構成的に与えた点に，本研究の有効性がある．

(2) マルチユーザ通信路における多項式時間で復号可能な符号化法の拡張

複数の送信機とひとつの受信機から構成される多重アクセス通信路に対して，ステップ(1)で開発した連接符号化法の改良を行った．特に，内部符号も構成的に与える手法を開発した．これにより，連接符号化の全過程にわたって，確定的な構成法となる[学会発表 6]．また，連接符号化において，符号長 N に対して**線形オーダ**の時間計算量で復号を実行できる誤り訂正符号を外部符号に採用することにより，連接符号の全体の復号計算量も符号長 N の線形オーダで実行できることを示した．また，複数の受信機が存在する複合多重アクセス通信路においても，同様の性能が達成できることが分かった．これらの結果より，符号器数・復号器数がともに増加しても，同様な性能を持つ符号を構成的に与

えられると期待できる．さらに，干渉通信路においても同様な性能を持つ符号の構成法の基礎的な道具になると期待される．

(3) 多重アクセス通信路における有限ブロック長の最適符号の性能評価

多重アクセス通信路における符号化に対して，**有限長レート解析**のアプローチにより，符号長が有限のときに誤り率 ε を達成できる最大符号化レートを理論的に解析した[学会発表 2]．特に，従来よりも詳細な復号誤り確率の上界式と下界式を示した．これらは現在知られている誤り率の限界式の中で最も厳密であり，有限長符号に対する符号化レートの理論限界を特徴づけた点に意義がある．これにより，よりよい復号性能を持つ復号アルゴリズムの開発に繋がると期待している．

ここで扱った多重アクセス通信路は，各符号器が観測するメッセージ間に相関がある場合も含んでいる．これは，情報源・通信路の同時符号化の問題に相当する．したがって，マルチユーザシステムにおける**情報源符号化問題**の解析にも応用することが可能である．

(4) その他の主な研究成果

線形符号のクラスは符号長 N の 2 次多項式のオーダで符号化が可能な，通信路符号のクラスである．現在，実用化されている通信路符号のほとんどは線形符号のクラスに属する．したがって，最尤復号など強力な復号法を仮定した元で，線形符号の性能を詳細に解析することは，情報理論・符号理論の重要なテーマの一つである．本研究では，特に符号化レートが低い場合（**低レート領域**）に注目し，具体的な線形符号が達成できる復号誤り率の上界を示した[学会発表 7]．この上界式は，注目する符号の重み分布が分かれば，最適符号の性能からの差分を評価できる．さらにこの誤り率の評価方法を，信頼できない復号結果の時には復号不能のフラグを出力する**一般化復号法**を用いた場合，および複数の推定結果をリスト形式で出力する**リスト復号**を用いた場合の性能評価に拡張した[雑誌論文 1]．

盗聴者が存在する通信システム（**盗聴通信路**）において，補助者が存在する時に達成できる符号化レートの領域を改善する方法を提案した[学会発表 5]．これはユーザ間協調通信の情報セキュリティへの応用と見ることができ，協調者の存在により送信メッセージの秘匿性を保ったまま通信効率が改善できることを示している．

マルチメディアコンテンツの著作権保護を目的とした**デジタル指紋符号化**システムは『符号器協調を許容する多重アクセス通信路』としてモデル化でき，両システムは密接な関係にある．多重アクセス通信路と類似したデジタル指紋符号化システムに対し，連接符号化とリスト復号法を組み合わせることにより，符号長に対して多項式時間の計算量で不正者が検出できるアルゴリズムを開発し，全ての不正者が正しく検出できる符号パラメータの十分条件を示した[雑誌論文 3]．また，不正者によって検出される確率に差がでない（公平な）攻撃を仮定し，安全性を保証した元で達成できるユーザ数レートの上限を示した[学会発表 1]．

５．主な発表論文等

〔雑誌論文〕（計 5 件）

[1] H. Yagi, H. V. Poor, "Bounds on maximum likelihood decoding performance for linear codes at low rates," （査読あり） IEEE Trans. Information Theory, vol.59, no.5, 2013 年 3 月(採録決定).
DOI: 10.1109/TIT.2013.2252394

[2] G. Hosoya, H. Yagi, M. Kobayashi, S. Hirasawa, "On the capacity of fingerprinting codes against AND, averaging, and related attacks," (査読あり) Journal of Information Assurance and Security, vol.7, pp. 41-51, 2012 年 5 月.
URL: http://www.mirlabs.net/jias/secured/Volume7-Issue1/vol7-issue1.html

[3] H. Yagi, T. Kawabata, "Polynomial-time codes against averaging attack for multimedia fingerprinting," （査読あり） Multimedia–A Multidisciplinary Approach to Complex Issues, InTech., 2012 年 2 月.
DOI: 10.5772/35316

[4] H. Yagi, H. V. Poor, "Coset codes for compound multiple access channels with common information," （査読あり） IEEE Trans. Information Theory, vol.57, no.6, pp. 3429-3448, 2011 年 6 月.
DOI: 0.1109/TIT.2011.2132570

[5] H. Yagi, H. V. Poor, "Polynomial-time decodable codes for multiple access channels," （査読あり） IEEE Commun. Letters, vol.15, no.1, pp. 73-75, 2011 年 1 月.
DOI: 10.1109/LCOMM.2010.120610.101847

〔学会発表〕（計 7 件）

[1] T. Narita, H. Yagi, T. Kawabata, "Analysis on the fingerprinting capacity for memoryless and fair collusion

attacks," (査読あり) Proc. of 2013 RISP Int. Workshop on Nonlinear Circuits, Communications and Signal Processing (NCSP2013), Hawaii, USA, 2013年3月.
[2] H. Yagi, "Finite blocklength bounds for multiple access channels with correlated sources," (査読あり) Proc. Int. Symp. on Information Theory and its Applications (ISITA2012), pp.377-381, Hawaii, USA, 2012年10月.
[3] B. M. Kurkoski, H. Yagi, "Finding the capacity of a quantized binary-input DMC," (査読あり) Proc. of 2012 IEEE Int. Symposium on Information Theory (ISIT2012), pp.691-695, Boston, USA, 2012年7月.
[4] H. Yagi, B. M. Kurkoski, "Channel quantizers that maximize random coding exponents for binary-input memoryless channels," (査読あり) Proc. of 2012 IEEE Int. Conf. on Communications (ICC2012), pp.2256-2260, Ottawa, Canada, 2012年6月.
[5] N. Marina, H. Yagi, H. V. Poor, "Improved rate-equivocation regions for secure cooperative communication", (査読あり) Proc. of 2011 IEEE Int. Symp. on Information Theory (ISIT2011), pp.2832-2836, St. Petersburg, Russia, 2011年8月5日.
[6] H. Yagi, H. V. Poor, "An explicit construction of concatenated codes for multiple access channels", (査読あり) Proc. of Forty-Eighth Annual Allerton Conference on Communication, Control, and Computing, IL, USA, 2010年9月.
[7] H. Yagi, H. V. Poor, "Performance an alysis of linear codes under maximum likelihood decoding at low rates", (査読あり) Proc. of 2010 IEEE Int. Symp. o n Information Theory (ISIT2010), pp.11 68-1172, Austin, USA, 2010年6月.
[8] H. Yagi, H. V. Poor, "Coset codes for multiple access channels with common information based on LDPC codes", (査読あり) Proc. of 2010 IEEE Int. Symp. on Information Theory (ISIT2010), pp.475-479, Austin, USA, 2010年6月.

６．研究組織

(1)研究代表者

八木 秀樹（YAGI HIDEKI）
電気通信大学・大学院情報理工学研究科・准教授
研究者番号：60409737